USAWC STRATEGY RESEARCH PROJECT

# DOMINATING CYBERSPACE

by

Commander Richard A. Radice
United States Navy

Dr. Doug Johnson
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **30 MAR 2007** | **Strategy Research Project** | **00-00-2006 to 00-00-2007** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Dominating Cyberspace** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| **Richard Radice** | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050** | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**See attached.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | | **17** | |

## ABSTRACT

AUTHOR: Commander Richard A. Radice

TITLE: Dominating Cyberspace

FORMAT: Strategy Research Project

DATE: 12 March 2007 WORD COUNT: 5000 PAGES: 17

KEY TERMS: Battlespace; Domain; Commons; Spectrum of Conflict

CLASSIFICATION: Unclassified

This paper explores how the military can establish 'cyber-dominance' in the battlespace of today and in the future. Cyberspace has its own challenges as an arena in which to conduct warfare just like land, sea, air and space do. This poses common problems to each of the services and the future of joint warfare. This paper will discuss the elements of battlespace dominance as they relate to the cyberspace domain in the near future and recommends how the joint force can organize itself to remain preeminent.

# DOMINATING CYBERSPACE

The future is now and the consequence for not seizing the initiative in cyberspace will be irrelevance. Computer networks, the internet, cell phones, and portable media are just some of the elements that comprise the interconnected cyberspace infrastructure that can exchange and manipulate information at a nearly instantaneous rate. We can not foresee all of the innovations that will shape this domain in the years to come, but the fact remains that its limitations are only bounded by our own imaginations and it continues to grow at speeds, and in directions, that few will be able to predict. The military must innovate itself, not just technologically, but as an organization in order to be effective on the future battlefield.

This paper will define relevant cyberspace and battlespace dominance terms, relating them together as a framework for recommending how the future joint force should organize to fight. Exploring dominance in cyberspace will include determining the greater benefits to friendly commanders and how the domain can be exploited to defeat the enemy. Cyberspace is different from the other domains. There are advantages that can be leveraged and the force conducting these operations should be organized to fully realize their potential and grow as the domain evolves.

## Background

The term cyberspace was coined by William Gibson in his 1984 science fiction novel *Neuromancer*.[1] It has grown from a writer's concept into a worldwide phenomenon that encompasses more than was originally conceived. Viewing cyberspace as strictly a technical system allows for an understanding of how it operates and leads to many common definitions, including one from our *National Strategy to Secure Cyberspace*: "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[2] Joint doctrine defines cyberspace more broadly as "the notional environment in which digitized information is communicated over computer networks."[3]

The real power inherent in the cyber domain derives from the myriad of new ways that people use it to achieve specific goals and objectives. Unlike the air, land, maritime and space commons, cyberspace's physical boundaries are not rigid and have no theoretical limitations. This allows the characteristics for operating in cyberspace to evolve rapidly and to be bounded only by the user's ability to imagine. Defense against cyber-attacks can be difficult, but will have measurable results. "We can't touch or see cyberspace, but we can see the results of things that happen in cyberspace—continuation of essential services or the degradation of those

services."[4] Services that rely on cyberspace may include national strategic interests like electrical power grids, operational systems like a common operating picture encompassing multiple major battle spaces in a theater, or tactical information exchange networks.

Information is the valuable commodity of cyberspace. The technical infrastructure determines the speed and scope of distribution, but people will continue to determine how it is packaged and presented in order to impact targeted audiences and achieve desired effects. Worldwide audiences can be addressed quickly by any individual, or group, with access. Joint doctrine defines information operations to be:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[5]

While the definitions of cyberspace and information operations overlap, neither should be considered a subset of the other. Both are heavily interrelated and apply to the full spectrum of operations. This paper uses the broader *Joint Doctrine* definition of cyberspace to explore what it means to establish cyber dominance on the Twenty-First Century Battlefield. This definition will be more applicable to future warfare as the cyber commons continues to mature, equating it more closely with the other global commons than with information operations. The potential growth of cyberspace warrant it being decoupled from information operations in the future and considered its own domain, requiring offensive and defensive consideration by commanders attempting to establish full spectrum dominance.

Battlespace dominance is doctrinally defined as "the degree of control over the dimensions of the battlespace that enhances friendly freedom of action and denies the enemy freedom of action. It permits power projection and force sustainment to accomplish the full range of potential missions."[6] Battlespace is "all aspects of air, surface, and subsurface, land, space and the electromagnetic spectrum that encompass the area of influence and area of interest."[7] Doctrine further defines the area of influence as "a geographical area in which a commander is directly capable of influencing operations by maneuver or fire support"[8] and the area of interest as "that area of concern to the commander, including the area of influence, areas adjacent, and areas extending into enemy waters or territory to the objectives of current or planned operations. This also includes areas occupied by enemy forces that could jeopardize the mission."[9] Using this battlespace framework helps define what dominance in cyberspace is.

Cyber Dominance

How cyberspace fits into the definition of battlespace derives from how it applies to the areas of influence and interest. Unlike land, air, sea and space, which are geographically bounded, the limits of cyberspace are always changing and differ from the electromagnetic spectrum because operations in all of the commons increasingly depend on it. Cyberspace facilitates new versions of fire and maneuver that take advantage of the unique networked environment in which future war will be waged.

Cyberspace operations are essential both directly and indirectly in the commander's area of influence. Indirect support of the other warfare specialties includes uses as a means of communications and information exchange. By protecting the friendly use of cyberspace, the commander enhances coordination, enables maneuver and increases the effectiveness of fires throughout the full spectrum of warfighting. Cyberspace also provides a unique means for conducting intelligence, surveillance, and reconnaissance (ISR) to assess an opponent's composition, disposition, and intentions; as well as provide indications and warnings (I&W) of planned attacks. Gathering background information to learn about the concerns and interests of any non-combatants in the battlespace can help shape the commander's perspective. Direct influence in the cyber-battlespace can be through clandestine monitoring, infiltration of an opponents organization by impersonating a member, cyber-attacks that misdirect or deny an opponents use of cyberspace, or by kinetic disruption of the infrastructure that an opponent uses for cyber-access. (E.g.: Telecommunication centers; Cell phone towers; Internet hubs; Media centers; etc…)

Cyberspace provides the best means for a commander to quickly assess and analyze what is happening, allowing their area of interest to expand and improving situational awareness. Geographically, a networked common operating picture provides the commander with an understanding beyond their formation to include the movement of friendly forces in adjacent areas overlaid against the opponent's disposition in a near real-time display. Ideologically, as a commander seeks more information about an opponent or the operating environment, networks allow historical and background information to be gathered from organizations worldwide with little delay. Logistics connectivity provides greater visibility of forces available for additional maneuver, relief or reinforcement, and enhances the efficiency of supply support to ongoing operations. Planning efforts would experience fewer, and shorter, delays while waiting for required elements of friendly information, thereby allowing operations to advance at speeds determined by the tactical situation.

Most discussions address dominance's technical aspects, but it is important to realize that all cyber-operations must be coordinated in a coherent plan to achieve the nation's strategic vision. How is dominance established? Networking. In the broader definition, it includes the cyber-infrastructure, organizational structure and people.

> It takes networks to fight networks. Governments that want to defend against netwar may have to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for interagency and multi-jurisdictional cooperation.[10]

The first step to establishing dominance is securing cyberspace to assure friendly access and prevent unwanted interference or influence. For commanders in the field to fully utilize and take advantage of technological advances, these systems need to be reliable and free from an opponent's attack. "Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures."[11] It is not enough for future systems to be secure; their effectiveness will also be determined by their reliability and relevance. The commander should be able to access, display and transmit only desired information without delay, hassle or confusion. "To realize its potential, a fully interconnected network requires a capacity for constant, dense information and communications flows, more so than do other forms of organization."[12]

The second step is to organize and train friendly forces to best exploit technological advantages and adapt quickly to an opponent's changing tactics. This provides a distinct advantage when confronted with a conventional enemy, but it becomes imperative when battling an asymmetric enemy, like Al-Qaeda, who is organized into a global network that can simultaneously threaten multiple trans-national interests.

> This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for interagency and multi-jurisdictional cooperation.[13]

Globalization is going to increasingly test the ability of nations to focus on solutions coordinated among all the main elements of national power: diplomatic; information; military; economic; financial; intelligence; and law enforcement. Developing a networked interagency

process that can quickly adapt to counter changes in an enemy's tactics is the only way to defeat a non-state enemy that enjoys freedom of movement in the global commons and understands how to leverage cyberspace for coordination. This translates to flattening the traditionally hierarchical military organizations into a more networked force that can jointly respond to threats in their area of responsibility.

For commanders to fully benefit from access to vast amounts of information, it must be shared quickly, analyzed for relevance and packaged in an easily digestible format. The speed of exchanging information will be essential to stay ahead of a rapidly evolving environment and an enemy that can adapt and improvise. The information technology required to gather and disseminate relevant information already exists and will continue to improve for the foreseeable future. The analysis and presentation format of the information will continue to require human insight and supervision to ensure appropriateness and accuracy. Rather than clogging-up bandwidth with huge amounts of raw data or superfluous information, relevant information needs to be culled out, prioritized and disseminated in its most efficient form. While designers must conform to the commander's requirements, commanders must also curb their appetite for aesthetic "window dressing" that requires large amounts of bandwidth but does not provide additional information or insight.

For commanders to fully leverage information superiority toward the goal of achieving cyber-dominance, they must seamlessly interact together to adapt faster than the changing environment. This can be achieved by flattening the operational military organization to increase efficiency, without sacrificing oversight, and provide subordinate commanders with adequate guidance and the freedom to exercise initiative. Shortening the chain of command down to the unit executing a mission may ruffle some traditionalist feathers and reduce the number of experienced reviewers for guidance and planning, but increasing the speed of execution should be worth the risk. For example, a ship could be assigned to a high-profile security mission reporting directly to the Joint Forces Maritime Component Commander (JFMCC), bypassing the usual squadron, group and fleet affiliations, to speed the communication of JFMCC's authorization for time critical actions. This reduces two or three levels of command and speeds response time to the fighting unit who must respond in a crisis.

Extending the example will demonstrate the benefit of networking horizontally across the organization. Assume the same ship's security mission operating area is in a near-shore region that forms a barrier between heavy surface traffic from which an attack is anticipated and a high value unit that may be a target. In the direction of the anticipated threat are three adjacent operating areas assigned to three different units: a mobile security squadron providing point

defense for gas and oil platforms inside territorial waters; a riverine squadron patrolling a river that empties into the region; and an infantry battalion responsible for security ashore including a small fishing village. The mobile security squadron works indirectly for the JFMCC through a task force commander while the riverine squadron and the infantry commander are both assigned to the same area commander who reports to the Joint Land Force Component Commander (JFLCC). Associated with each of these commands is a networked cell of a cyberspace command that is responsible for processing gathered information and distributing it on the network. Without violating their distinct chains of command, these four units can share information that seems innocuous to each individually, but when seen as a whole can provide enough warning to foil an asymmetrical attack. The cyber command cell will provide greater situational awareness. They could empower friendly units with geographical position displays that are both annotated to highlight anomalies and synchronized with a blog that provides amplifying information applicable to the region. These displays would be common and accessible by all units, regardless of their associated chains of command. This will enable them to piece together every indication, no matter how small, into a coherent warning of an opponent's intent faster than attacks can be executed or changed. As an example:

While identifying and randomly inspecting river traffic, the riverine squadron notes that several boats were slightly off their normal down river schedule but responded satisfactorily to queries, so they were allowed to proceed without inspection. The troops in the village note that more boats are remaining inport, yet the village is unusually quiet for that time of day and several boat arrivals are overdue. Alerted by the fact that the areas south of the platforms were clearing during a prime fishing time, the mobile security squadron's cyber cell scans the recent blog history noticing that several vessels were identical between the two above reports. They request if anyone has updated locating data and raises the squadron's alert condition against a possible attack. In response, the ship launches its helicopter and begins to reposition to the north where it can be ready to support the platforms. A separate element of the troops ashore reports that a vessel matching one of the suspect's descriptions is foundering off the coast well south of the platforms. While investigating this contact, the helicopter identifies a group a small vessels maneuvering in the direction the high-value asset. This warning ends up providing just enough time to reposition assets to determine the boats intent and defeat a possible attack.

If the three reports from the JFLCC units were required to be vetted through command chains, they would have been delivered too late to be correlated and alert the JFMCC units of the potential attack. Historically proven command relationships can remain unchanged, but to fully leverage cyberspace, friendly forces have to utilize a networked organization independent

from operational chains of command. This scenario crudely illustrated how it is just as important to provide information flatly across friendly networks, and train commanders to leverage it, as it is to ensure each friendly unit's access to the cyberspace domain.

The next step is to deny, or control, how and when opponents can access cyberspace. This is the most difficult task because emerging technologies mature quickly and our opponents learn fast to embrace these changes in innovative and unanticipated ways. "It is important to understand that this technology is not simply a communication tool; in large part, it is what makes a networked organization possible."[14] By attacking asymmetrical opponents in cyberspace, we are striking at the heart of their organizational structure. Even if a successful cyber-campaign does not collapse a networked opponent in total defeat, it will render a level of impotence that will prevent individual cells from launching coordinated attacks, greatly reducing their effectiveness. Conventional opponents suffer from cyberspace defeats differently. Their firepower retains its lethality, but by degrading their ability to communicate and coordinate within their organization, the speed at which they can maneuver and react is reduced, providing an advantage to the warrior that retains their use of cyberspace.

Attacks to deny an opponent the use of cyberspace can be either kinetic or non-kinetic. Kinetic methods generally involve destroying elements of an opponent's infrastructure or organization to cripple their ability to operate. Infrastructure targets could include communication centers, internet service providers or even satellites; and established tactics using various conventional weapons could be used. A weapon employing an electromagnetic pulse would be particularly effective against information technology, but being indiscriminate, it would also cause a great deal of collateral damage and require comprehensive protection of friendly systems. Capturing, killing, or isolating key planners and leaders will cause an organization to slow down and adapt. Networked opponents should be able react faster, requiring sustained sequential efforts to continue to eliminate key nodes. These same targets can be attacked non-kinetically using tactics that include: jamming signals in the electromagnetic spectrum, turning off telecommunications services through infiltration or interrupting power sources, and interrupting internet service using methods developed by hackers. Some of the commonly known hacks include: automated denial of service attacks, viruses, worms and trojan horses.

Controlling an opponent's use of cyberspace is a much more sophisticated and elegant solution that has the potential to be more effective. These techniques are most related to the conventional tactics of operational deception, meaconing, and clandestine surveillance. In the realm of cyber-crime, identity thieves search out vulnerable marks and then monitor their

activities in cyberspace to collect personal information, account numbers and passwords. Military surveillance in cyberspace can leverage similar techniques to search out enemies, and potential enemies, monitoring their activities to reveal their intentions, collaborators, tactics and location.

Locating and tracking an opponent in cyberspace is the first step in focusing deception and meaconing efforts against them. Using phishing techniques, also pioneered by cyber-criminals, it is possible to redirect an enemy from their desired website to a nearly identical one with information deliberately changed to help shape the enemy's actions to our advantage or employing methods to gather information from visitors. In addition: websites, blogs and chat rooms can be created to attract the enemy so they can be identified and tracked, or to further spread misinformation that disrupts enemy planning. Meaconing is using communications media to impersonate a member of the enemy organization and gather information to use in operations against them. The internet is already a playground for individuals to assume false identities and engage in relationships that would not normally be possible. Assuming an identity that is attractive to an opponent, frequenting the same chat rooms and blogs, and professing interest in their cause could help infiltrate enemy organizations as a new member. Against asymmetrical threats like terrorists, this may involve championing their cause or posing as a potential financial or equipment supporter. Conventional enemies may be looking for potential sources of intelligence to exploit. In either case, once the false identity is accepted by an opponent, it can be cultivated to build further trust and gather information about the enemy's intentions and possibly provide them false information to disrupt their overall strategy. The next level of meaconing involves using identity theft techniques to steal the identity of a known member of an enemy organization and then impersonate them in e-mails, chat rooms and possibly even on cell or telephones. The sophistication required for this to be successful includes fully understanding the targeted individual and mimicking the communication and encryption techniques of the organization to avoid discovery. The target must not be permitted to expose ongoing operations, requiring their isolation, elimination or by making their actions irrelevant.

Manipulating the enemy in cyberspace is not enough unless the analyzed information is efficiently organized and accessible by commanders at all levels without bureaucratic delays. Throughout planning, it is equally important that the first, second and third order effects of cyber-operations be coordinated across the friendly network to determine if they match the desired intentions of the affected commanders. Characteristics of the cyberspace domain make it possible for a single operation against a networked opponent to have worldwide implications

affecting all of the geographical combatant commanders' theater of operations. Networking a national information exchange approach can improve coordination during planning and accelerate response times as an operation's effects become realized.

Expanding our global networks to include an increasing number of countries from the international community can strengthen global security, broaden the scope of effort, and increase the effectiveness of everyone's participation. Globalization has irrevocably interlaced the interests and concerns of all the nations in the world, and its influence will only increase with time. It is mutually beneficial for countries to share the responsibility to act where the national interests of multiple countries overlap. Coordinating actions equally among participating nations allows for a more powerful response while each country only responds to what is in their nation's interest. An example is the global maritime network concept being championed by the United States Navy called the *1,000 Ship Navy*.[15] Networking from both an organizational framework and with an information exchange system is the key to dominating cyberspace, but what should it look like?

Recomendations

A combatant command should be created to conduct cyberspace operations in a similar way that the Special Operations Command (SOCOM) conducts irregular warfare. This special status is warranted because "the healthy functioning of cyberspace is essential to our economy and our national security."[16] As the twenty-first century continues, cyberspace will become the dominant commons and will continue to grow in size, complexity and importance. To remain relevant and secure in the global community, the United States must ensure it is preeminent in cyberspace and can defeat threats to global cyber-security. This requires that the new command be organized to be most effective in the cyber domain and its warriors be trained and equipped to fully leverage the evolving domain to support national interests.

The organization should be more network-styled rather than the traditional military hierarchy because the domain dictates greater flexibility and speed of action. A cyber-command must be responsive to the warfighters that it serves, from geographical and functional combatant commanders to the individual services and possibly even other governmental agencies. There are no accurate boundaries that would allow cyberspace to be divided along geographical lines similar to the sea, airspace, and land commons and it requires a coordinated effort throughout the domain if commanders fighting in the other commons are to be able to leverage it with confidence. Furthermore, the command responsible for cyberspace needs to keep pace with changes in technology and the innovative exploitation that define the commons;

and whenever possible lead that innovation. We can't afford to give our enemies the opportunity to shape the future battlespace for us.

> Most people might hope for the emergence of a new form of organization to be led by "good guys" who do "the right thing" and grow stronger because of it. But history does not support this contention. The cutting edge in the early rise of a new form may be found equally among malcontents, ne'er-do-wells, and clever opportunists eager to take advantage of new ways to maneuver, exploit, and dominate.[17]

To be responsive to customers, the command should be distributed into cells that are accessible by customers at all levels and collocated with critical users where possible. Commanders from the national, strategic, theater, operational and possible even tactical levels would be included, but the networked structure would not necessarily replicate their hierarchical chains of command. The greater the number and distribution of effective cells incorporated into the network, the greater the potential is dominate in cyberspace. Each cell would work directly with the commanders that they are supporting with a synergistic relationship that can not be duplicated through liaison officers, e-mail or message traffic. Together the cells would share information to build a worldwide operating picture that individual commanders can tailor to their needs. Cells will collectively fight threats to friendly access in a manner that is transparent to the commanders they support. Attacks against enemy uses of cyberspace would be distributed through the network to ensure that the appropriate cells are involved, with the potential that some cells be trained in specific attack tactics rather than support roles. Many cells geographical location will not have to be linked to their operational assignments.

Who would lead this networked organization for it to be effective in a bureaucratic government? The command should be organized into four levels: national; strategic; operational; and tactical. Within each level, cells should be considered equal in the network even if the cells' commanders are of different ranks. The national level would contain cells led by the commander and deputy commander that are responsible for supporting the commander-in-chief and all of the potential national command centers. The flag-led strategic cells would be aligned with theater and service level commanders while operational cells would be focused on specific large scale operations and led by an O-5 or O-6. The tactical cells would be the most diverse and organized not only to support a myriad of operations, but they would also consist of the cells that conduct cyber-attacks.

Manning should include personnel from throughout the defense, intelligence and law enforcement agencies while the funding for equipment and operations should be separate. (This funding arrangement would be similar to what exists now for SOCOM.) Drawing

personnel from the existing force allows selection of personnel with experience and demonstrated performance. Their tours should alternate between parent service assignments and those within the cyberspace command, enabling them to increase interoperability through shared knowledge and experience while maintaining their career progression. An increasing amount of training will be required as personnel progress in their careers. Training should be state of the art, taught by experts, and require a service commitment to ensure capitalization.

There will be difficulties merging a networked organization into the traditional bureaucratic and military structures while trying to gain acceptance within their existing cultures. Leaders must look beyond their comfort zone to create an evolving organization and empower it to develop in the same manner that cyberspace does, but hopefully at a slightly greater pace. The services have not embraced cyberspace as an equal domain and their approach so far has been parochial and tends to address specific aspects of cyberspace. Only the Air Force has formed a command focused on cyberspace,[18] time will tell if it remains locked into a traditional hierarchical structure and if it receives equal attention and acceptance within the service. For the force to fight jointly, we need to truly innovate across the services.

On a national scale, creating an interagency command with a relatively flat organizational structure and placing it in charge of coordinating efforts of all departments could be innovative enough to remain ahead of the future global environment for the next century and achieve the president's vision for the nation and its security. The command would primarily deal with the information element of national power, requiring operations in cyberspace to be completely complimentary. An honest information campaign, coordinated for accuracy, and quickly disseminated would be hard to effectively attack and nearly impossible to defeat. The State Department should provide a senior career Foreign Service ambassador as the commander with the other executive branch departments would contribute to round out the command structure.

## Conclusion

Cyberspace is quickly becoming the dominant commons and can continue to grow unbounded. Operations of every type, in all of the commons, rely heavily on the use of cyberspace. Dominating in this domain is important now and will become essential in the near future as other nations and transnational actors leverage their technical expertise and experience at increasingly greater rates. Establishing a combatant commander to coordinate operations in cyberspace will create the conditions necessary for the United States to dominate cyberspace whenever required.

Utilizing a relatively flat command structure organized in a networked fashion will ensure that the command can grow and innovate to keep pace with the rapid evolution of cyberspace while ensuring interoperability and swift support to operational forces. Mission oriented cells would ensure that individual commanders have the information they require to access their areas of interest and influence and that it is provided to them in the quickest and most relevant form. They would also provide a means for collecting and sharing information based on operational interest without parochial bias and enabling commanders in contact a greater freedom of action.

A cyber command can take the fight to the enemy through various methods of surveillance and attack, denying freedom of movement or cyber-cover to an opponent. "In the past few years Islamist websites have provided ample evidence that Islamist hackers do not operate as isolated individuals, but carry out coordinated attacks against websites belonging to those whom they regard as their enemies."[19] A networked organization will also be able to quickly detect, disseminate and counter changes in an opponent's operations and tactics, thereby maintaining dominance and giving operational forces an advantage on the battlefield. Bigger networks are harder to defend, but generate such a powerful and adaptable force that it is worth seeking to increase the size of the organization to include the other departments of the federal government, state organizations and even other countries. Cyberspace is going to be bigger and more important in the future than any of us can imagine. We need to organize now for future success before others seize the opportunity and make our participation irrelevant.

Endnotes

[1] William Gibson, *Neuromancer* (New York: Ace Books, 1984), 4.

[2] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington D.C.: The White House, February 2003), vii.

[3] Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington, D.C.: Joint Chiefs of Staff, 13 February 2006), GL-6.

[4] Arnold K. Veazie, *U.S. Strategy for Cyberspace*, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 07 April 2003), 1.

[5] Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington, D.C.: Joint Chiefs of Staff, 13 February 2006), GL-9.

[6] U.S. Department of the Navy, Naval Warfare, *Naval Doctrine Publication 1* (Washington, D.C.: Department of the Navy, 28 March 1994), 72.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] John Arquilla and David Ronfeldt, "The Advent of Netwar Revisted," in Networks and Netwars: The Future of Terror, Crime and Militancy, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), 15.

[11] George W. Bush, The National Strategy to Secure Cyberspace (Washington D.C.: The White House, February 2003), ix.

[12] Arquilla and Ronfeldt, *The Advent of Netwar Revisted*, 10.

[13] Ibid., 15.

[14] Martin J. Muckian, "Structural Vulnerabilities of Networked Insurgencies: Adapting to the New Adversary," Parameters, (Winter 2006-07): 22.

[15] Michael G. Mullin, *CNO Guidance for 2007* (Washington, D.C.: Department of the Navy, 02 February 2007), 5.

[16] George W. Bush, The National Strategy to Secure Cyberspace (Washington D.C.: The White House, February 2003), vii.

[17] David Ronfeldt and John Arquilla, "What Next for Networks and Netwars?," in Networks and Netwars: The Future of Terror, Crime and Militancy, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), 313.

[18] John C.K. Daly, "US Air Force Prepares For Cyber Warfare," *SPACEWAR: Your World at War*, 09 October 2006 [journal on-line] available from http://www.spacewar.com/ reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html; accessed 20 October 2006.

[19] E. Alshech, "Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad," *The Middle East Media Research Institute Inquiry and Analysis Series Number 329*, 27 February 2007 [journal on-line] available from http://www.memri.org/bin/opener_latest.cgi?ID=IA32907; accessed 11 March 2007.